

# Foundation of Cryptography, Lecture 3

## Hardcore Predicates for Any One-way Function

Iftach Haitner, Tel Aviv University

Tel Aviv University.

March 4, 2014

## Informal Discussion

$f$  is one-way  $\implies$  predicting  $x$  from  $f(x)$  is hard.

## Informal Discussion

$f$  is one-way  $\implies$  predicting  $x$  from  $f(x)$  is hard.

But predicting parts of  $x$  might be easy.

## Informal Discussion

$f$  is one-way  $\implies$  predicting  $x$  from  $f(x)$  is hard.

But predicting parts of  $x$  might be easy.

e.g., let  $f$  be a OWF then  $g(x, w) = (f(x), w)$  is one-way

## Informal Discussion

$f$  is one-way  $\implies$  predicting  $x$  from  $f(x)$  is hard.

But predicting parts of  $x$  might be easy.

e.g., let  $f$  be a OWF then  $g(x, w) = (f(x), w)$  is one-way

Can we find a function of  $x$  that is totally unpredictable — looks uniform — given  $f(x)$ ?

## Informal Discussion

$f$  is one-way  $\implies$  predicting  $x$  from  $f(x)$  is hard.

But predicting parts of  $x$  might be easy.

e.g., let  $f$  be a OWF then  $g(x, w) = (f(x), w)$  is one-way

Can we find a function of  $x$  that is totally unpredictable — looks uniform — given  $f(x)$ ?

Such functions have many cryptographic applications

# Formal Definition

## Definition 1 (hardcore predicates)

A poly-time computable  $b: \{0, 1\}^n \mapsto \{0, 1\}$  is an **hardcore predicate** of  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$ , if

$$\Pr_{x \leftarrow \{0,1\}^n} [P(f(x)) = b(x)] \leq \frac{1}{2} + \text{neg}(n)$$

for any PPT  $P$ .

# Formal Definition

## Definition 1 (hardcore predicates)

A poly-time computable  $b: \{0, 1\}^n \mapsto \{0, 1\}$  is an **hardcore predicate** of  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$ , if

$$\Pr_{x \leftarrow \{0, 1\}^n} [P(f(x)) = b(x)] \leq \frac{1}{2} + \text{neg}(n)$$

for any PPT  $P$ .

- Does any OWF has such a predicate?



# Formal Definition

## Definition 1 (hardcore predicates)

A poly-time computable  $b: \{0, 1\}^n \mapsto \{0, 1\}$  is an **hardcore predicate** of  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$ , if

$$\Pr_{x \leftarrow \{0, 1\}^n} [P(f(x)) = b(x)] \leq \frac{1}{2} + \text{neg}(n)$$

for any PPT  $P$ .

- Does any OWF has such a predicate?
- Is there a **generic** hardcore predicate for all one-way functions?

# Formal Definition

## Definition 1 (hardcore predicates)

A poly-time computable  $b: \{0, 1\}^n \mapsto \{0, 1\}$  is an **hardcore predicate** of  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$ , if

$$\Pr_{x \leftarrow \{0,1\}^n} [P(f(x)) = b(x)] \leq \frac{1}{2} + \text{neg}(n)$$

for any PPT  $P$ .

- Does any OWF has such a predicate?
- Is there a **generic** hardcore predicate for all one-way functions?

Let  $f$  be a OWF and let  $b$  be a predicate, then  $g(x) = (f(x), b(x))$  is one-way.

# Formal Definition

## Definition 1 (hardcore predicates)

A poly-time computable  $b: \{0, 1\}^n \mapsto \{0, 1\}$  is an **hardcore predicate** of  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$ , if

$$\Pr_{x \leftarrow \{0,1\}^n} [P(f(x)) = b(x)] \leq \frac{1}{2} + \text{neg}(n)$$

for any PPT  $P$ .

- Does any OWF has such a predicate?
- Is there a **generic** hardcore predicate for all one-way functions?

Let  $f$  be a OWF and let  $b$  be a predicate, then  $g(x) = (f(x), b(x))$  is one-way.

- Does the existence of hardcore predicate for  $f$  implies that  $f$  is one-way?

# Formal Definition

## Definition 1 (hardcore predicates)

A poly-time computable  $b: \{0, 1\}^n \mapsto \{0, 1\}$  is an **hardcore predicate** of  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$ , if

$$\Pr_{x \leftarrow \{0,1\}^n} [P(f(x)) = b(x)] \leq \frac{1}{2} + \text{neg}(n)$$

for any PPT  $P$ .

- Does any OWF has such a predicate?
- Is there a **generic** hardcore predicate for all one-way functions?

Let  $f$  be a OWF and let  $b$  be a predicate, then  $g(x) = (f(x), b(x))$  is one-way.

- Does the existence of hardcore predicate for  $f$  implies that  $f$  is one-way?  
Consider  $f(x, y) = x$ , then  $b(x, y) = y$  is a hardcore predicate for  $f$

# Formal Definition

## Definition 1 (hardcore predicates)

A poly-time computable  $b: \{0, 1\}^n \mapsto \{0, 1\}$  is an **hardcore predicate** of  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$ , if

$$\Pr_{x \leftarrow \{0,1\}^n} [P(f(x)) = b(x)] \leq \frac{1}{2} + \text{neg}(n)$$

for any PPT  $P$ .

- Does any OWF has such a predicate?
- Is there a **generic** hardcore predicate for all one-way functions?

Let  $f$  be a OWF and let  $b$  be a predicate, then  $g(x) = (f(x), b(x))$  is one-way.

- Does the existence of hardcore predicate for  $f$  implies that  $f$  is one-way?

Consider  $f(x, y) = x$ , then  $b(x, y) = y$  is a hardcore predicate for  $f$

Answer to above is **positive**, in case  $f$  is **one-to-one**

# Weak Hardcore Predicates

## Weak Hardcore Predicates

For  $x \in \{0, 1\}^n$  and  $i \in [n]$ , let  $x_i$  be the  $i$ 'th bit of  $x$ .

## Weak Hardcore Predicates

For  $x \in \{0, 1\}^n$  and  $i \in [n]$ , let  $x_i$  be the  $i$ 'th bit of  $x$ .

### Theorem 2

For  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$ , define  $g: \{0, 1\}^n \times [n] \mapsto \{0, 1\}^n \times [n]$  by

$$g(x, i) = (f(x), i)$$

Assuming  $f$  is one way, then

$$\Pr_{x \leftarrow \{0, 1\}^n, i \leftarrow [n]} [A(f(x), i) = x_i] \leq 1 - 1/2n$$

for any PPT  $A$ .



## Weak Hardcore Predicates

For  $x \in \{0, 1\}^n$  and  $i \in [n]$ , let  $x_i$  be the  $i$ 'th bit of  $x$ .

### Theorem 2

For  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$ , define  $g: \{0, 1\}^n \times [n] \mapsto \{0, 1\}^n \times [n]$  by

$$g(x, i) = f(x), i$$

Assuming  $f$  is one way, then

$$\Pr_{x \leftarrow \{0, 1\}^n, i \leftarrow [n]} [A(f(x), i) = x_i] \leq 1 - 1/2n$$

for any PPT  $A$ .

Proof: ?

## Weak Hardcore Predicates

For  $x \in \{0, 1\}^n$  and  $i \in [n]$ , let  $x_i$  be the  $i$ 'th bit of  $x$ .

### Theorem 2

For  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$ , define  $g: \{0, 1\}^n \times [n] \mapsto \{0, 1\}^n \times [n]$  by

$$g(x, i) = f(x), i$$

Assuming  $f$  is one way, then

$$\Pr_{x \leftarrow \{0, 1\}^n, i \leftarrow [n]} [A(f(x), i) = x_i] \leq 1 - 1/2n$$

for any PPT  $A$ .

Proof: ?

We can now construct an hardcore predicate “for”  $f$ :

- 1 Construct a weak hardcore predicate for  $g$  (i.e.,  $b(x, i) := x_i$ ).
- 2 Amplify it into a (strong) hardcore predicate for  $g^t$  via parallel repetition

## Weak Hardcore Predicates

For  $x \in \{0, 1\}^n$  and  $i \in [n]$ , let  $x_i$  be the  $i$ 'th bit of  $x$ .

### Theorem 2

For  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$ , define  $g: \{0, 1\}^n \times [n] \mapsto \{0, 1\}^n \times [n]$  by

$$g(x, i) = f(x), i$$

Assuming  $f$  is one way, then

$$\Pr_{x \leftarrow \{0,1\}^n, i \leftarrow [n]} [A(f(x), i) = x_i] \leq 1 - 1/2n$$

for any PPT  $A$ .

Proof: ?

We can now construct an hardcore predicate “for”  $f$ :

- 1 Construct a weak hardcore predicate for  $g$  (i.e.,  $b(x, i) := x_i$ ).
- 2 Amplify it into a (strong) hardcore predicate for  $g^t$  via parallel repetition

The resulting predicate is not for  $f$  but for (the one-way function)  $g^t$  ...

# The Goldreich-Levin Hardcore predicate

For  $x, r \in \{0, 1\}^n$ , let  $\langle x, r \rangle_2 := (\sum_{i=1}^n x_i \cdot r_i) \bmod 2 = \bigoplus_{i=1}^n x_i \cdot r_i$ .

# The Goldreich-Levin Hardcore predicate

For  $x, r \in \{0, 1\}^n$ , let  $\langle x, r \rangle_2 := (\sum_{i=1}^n x_i \cdot r_i) \bmod 2 = \bigoplus_{i=1}^n x_i \cdot r_i$ .

## Theorem 3 (Goldreich-Levin)

For  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$ , define  $g: \{0, 1\}^n \times \{0, 1\}^n \mapsto \{0, 1\}^n \times \{0, 1\}^n$  as  $g(x, r) = (f(x), r)$ .

If  $f$  is one-way, then  $b(x, r) := \langle x, r \rangle_2$  is an hardcore predicate of  $g$ .

# The Goldreich-Levin Hardcore predicate

For  $x, r \in \{0, 1\}^n$ , let  $\langle x, r \rangle_2 := (\sum_{i=1}^n x_i \cdot r_i) \bmod 2 = \bigoplus_{i=1}^n x_i \cdot r_i$ .

## Theorem 3 (Goldreich-Levin)

For  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$ , define  $g: \{0, 1\}^n \times \{0, 1\}^n \mapsto \{0, 1\}^n \times \{0, 1\}^n$  as  $g(x, r) = (f(x), r)$ .

If  $f$  is one-way, then  $b(x, r) := \langle x, r \rangle_2$  is an hardcore predicate of  $g$ .

- Note that if  $f$  is one-to-one, then so is  $g$ .

# The Goldreich-Levin Hardcore predicate

For  $x, r \in \{0, 1\}^n$ , let  $\langle x, r \rangle_2 := (\sum_{i=1}^n x_i \cdot r_i) \bmod 2 = \bigoplus_{i=1}^n x_i \cdot r_i$ .

## Theorem 3 (Goldreich-Levin)

For  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$ , define  $g: \{0, 1\}^n \times \{0, 1\}^n \mapsto \{0, 1\}^n \times \{0, 1\}^n$  as  $g(x, r) = (f(x), r)$ .

If  $f$  is one-way, then  $b(x, r) := \langle x, r \rangle_2$  is an hardcore predicate of  $g$ .

- Note that if  $f$  is one-to-one, then so is  $g$ .
- A slight cheat,  $b$  is defined for  $g$  and not for the original OWF  $f$

# The Goldreich-Levin Hardcore predicate

For  $x, r \in \{0, 1\}^n$ , let  $\langle x, r \rangle_2 := (\sum_{i=1}^n x_i \cdot r_i) \bmod 2 = \bigoplus_{i=1}^n x_i \cdot r_i$ .

## Theorem 3 (Goldreich-Levin)

For  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$ , define  $g: \{0, 1\}^n \times \{0, 1\}^n \mapsto \{0, 1\}^n \times \{0, 1\}^n$  as  $g(x, r) = (f(x), r)$ .

If  $f$  is one-way, then  $b(x, r) := \langle x, r \rangle_2$  is an hardcore predicate of  $g$ .

- Note that if  $f$  is one-to-one, then so is  $g$ .
- A slight cheat,  $b$  is defined for  $g$  and not for the original OWF  $f$



# The Goldreich-Levin Hardcore predicate

For  $x, r \in \{0, 1\}^n$ , let  $\langle x, r \rangle_2 := (\sum_{i=1}^n x_i \cdot r_i) \bmod 2 = \bigoplus_{i=1}^n x_i \cdot r_i$ .

## Theorem 3 (Goldreich-Levin)

For  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$ , define  $g: \{0, 1\}^n \times \{0, 1\}^n \mapsto \{0, 1\}^n \times \{0, 1\}^n$  as  $g(x, r) = (f(x), r)$ .

If  $f$  is one-way, then  $b(x, r) := \langle x, r \rangle_2$  is an hardcore predicate of  $g$ .

- Note that if  $f$  is one-to-one, then so is  $g$ .
- A slight cheat,  $b$  is defined for  $g$  and not for the original OWF  $f$

Proof by reduction: a PPT  $A$  for predicting  $b(x, r)$  “too well” from  $(f(x), r)$ , implies an inverter for  $f$

# Section 1

## **Proving GL – The Information Theoretic Case**

# Min entropy

## Definition 4 (min-entropy)

The **min entropy** of a random variable (or distribution)  $X$ , is defined as

$$H_{\infty}(X) := \min_{y \in \text{Supp}(X)} \log \frac{1}{\Pr_X[y]}.$$

# Min entropy

## Definition 4 (min-entropy)

The **min entropy** of a random variable (or distribution)  $X$ , is defined as

$$H_{\infty}(X) := \min_{y \in \text{Supp}(X)} \log \frac{1}{\Pr_X[y]}.$$

Examples:

- $Z$  is uniform over a set of size  $2^k$ .
- $Z = X \mid_{f(X)=y}$ , where  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$  is  $2^k$  to 1 ,  
 $y \in f(\{0, 1\}^n) := \{f(x) : x \in \{0, 1\}^n\}$  and  $X$  is uniform over  $\{0, 1\}^n$ .

In both cases,  $H_{\infty}(Z) = k$ .

# Pairwise independent hashing

## Definition 5 (pairwise independent function family)

A function family  $\mathcal{H} = \{h: \{0, 1\}^n \mapsto \{0, 1\}^m\}$  is **pairwise independent**, if  $\forall x \neq x' \in \{0, 1\}^n$  and  $y, y' \in \{0, 1\}^m$ , it holds that  $\Pr_{h \leftarrow \mathcal{H}}[h(x) = y \wedge h(x') = y'] = 2^{-2m}$ .

# Pairwise independent hashing

## Definition 5 (pairwise independent function family)

A function family  $\mathcal{H} = \{h: \{0, 1\}^n \mapsto \{0, 1\}^m\}$  is **pairwise independent**, if  $\forall x \neq x' \in \{0, 1\}^n$  and  $y, y' \in \{0, 1\}^m$ , it holds that  $\Pr_{h \leftarrow \mathcal{H}}[h(x) = y \wedge h(x') = y'] = 2^{-2m}$ .

## Lemma 6 (leftover hash lemma)

Let  $X$  be a rv over  $\{0, 1\}^n$  with  $H_\infty(X) \geq k$  and let  $\mathcal{H} = \{h: \{0, 1\}^n \mapsto \{0, 1\}^m\}$  be pairwise independent, then

$$\text{SD}((H, H(X)), (H, U_m)) \leq 2^{(m-k-2)/2},$$

where  $H$  is uniformly distributed over  $\mathcal{H}$  and  $U_m$  is uniformly distributed over  $\{0, 1\}^m$ .

# Efficient function families

## Definition 7 (efficient function families)

An ensemble of function families  $\mathcal{F} = \{\mathcal{F}_n\}_{n \in \mathbb{N}}$  is **efficient**, if

**Samplable.** Exists PPT that given  $1^n$ , outputs (the description of) a uniform element in  $\mathcal{F}_n$ .

**Efficient.** Exists poly-time algorithm that given  $x \in \{0, 1\}^n$  and (a description of)  $f \in \mathcal{F}_n$ , outputs  $f(x)$ .

# Proving GL for compressing functions

## Definition 8

Function  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$  is  $d(n)$  regular, if  $|f^{-1}(y)| = d(n)$  for every  $y \in f(\{0, 1\}^n)$ .



# Proving GL for compressing functions

## Definition 8

Function  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$  is  $d(n)$  **regular**, if  $|f^{-1}(y)| = d(n)$  for every  $y \in f(\{0, 1\}^n)$ .

## Lemma 9

Let  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$  be a  $d(n) \in 2^{\omega(\log n)}$  regular function, and let  $\mathcal{H} = \{\mathcal{H}_n\}$  be an efficient family of Boolean pairwise independent functions over  $\{0, 1\}^n$ . Define  $g: \{0, 1\}^n \times \mathcal{H}_n \mapsto \{0, 1\}^n \times \mathcal{H}_n$  as

$$g(x, h) = (f(x), h),$$

then  $b(x, h) = h(x)$  is an hardcore predicate of  $g$ .

# Proving GL for compressing functions

## Definition 8

Function  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$  is  $d(n)$  **regular**, if  $|f^{-1}(y)| = d(n)$  for every  $y \in f(\{0, 1\}^n)$ .

## Lemma 9

Let  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$  be a  $d(n) \in 2^{\omega(\log n)}$  regular function, and let  $\mathcal{H} = \{\mathcal{H}_n\}$  be an efficient family of Boolean pairwise independent functions over  $\{0, 1\}^n$ . Define  $g: \{0, 1\}^n \times \mathcal{H}_n \mapsto \{0, 1\}^n \times \mathcal{H}_n$  as

$$g(x, h) = (f(x), h),$$

then  $b(x, h) = h(x)$  is an hardcore predicate of  $g$ .

How does it relate to Goldreich-Levin?

# Proving GL for compressing functions

## Definition 8

Function  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$  is  $d(n)$  **regular**, if  $|f^{-1}(y)| = d(n)$  for every  $y \in f(\{0, 1\}^n)$ .

## Lemma 9

Let  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$  be a  $d(n) \in 2^{\omega(\log n)}$  regular function, and let  $\mathcal{H} = \{\mathcal{H}_n\}$  be an efficient family of Boolean pairwise independent functions over  $\{0, 1\}^n$ . Define  $g: \{0, 1\}^n \times \mathcal{H}_n \mapsto \{0, 1\}^n \times \mathcal{H}_n$  as

$$g(x, h) = (f(x), h),$$

then  $b(x, h) = h(x)$  is an hardcore predicate of  $g$ .

How does it relate to Goldreich-Levin?

$\{\mathcal{H}_n = \{b_r(\cdot) = b(r, \cdot)\}_{r \in \{0, 1\}^n}\}$  is (almost) pairwise independent.

## Proving Lemma 9

The lemma follows by the next claim:

### Claim 10

$SD((f(U_n), H, H(U_n)), (f(U_n), H, U_1)) = \text{neg}(n)$ , where  $H = H_n$  is uniformly distributed over  $\mathcal{H}_n$ .

## Proving Lemma 9

The lemma follows by the next claim:

### Claim 10

$SD((f(U_n), H, H(U_n)), (f(U_n), H, U_1)) = \text{neg}(n)$ , where  $H = H_n$  is uniformly distributed over  $\mathcal{H}_n$ .

Proving the claim. For  $y \in f(\{0, 1\}^n)$ , let  $X_y$  be uniformly distributed over  $f^{-1}(y) := \{x \in \{0, 1\}^n : f(x) = y\}$ .

## Proving Lemma 9

The lemma follows by the next claim:

### Claim 10

$SD((f(U_n), H, H(U_n)), (f(U_n), H, U_1)) = \text{neg}(n)$ , where  $H = H_n$  is uniformly distributed over  $\mathcal{H}_n$ .

Proving the claim. For  $y \in f(\{0, 1\}^n)$ , let  $X_y$  be uniformly distributed over  $f^{-1}(y) := \{x \in \{0, 1\}^n : f(x) = y\}$ . Compute

$$\begin{aligned} &SD((f(U_n), H, H(U_n)), (f(U_n), H, U_1)) \\ &= \sum_{y \in f(\{0, 1\}^n)} \Pr[f(U_n) = y] \cdot \\ &\quad SD((f(U_n), H, H(U_n) \mid f(U_n) = y), (f(U_n), H, U_1 \mid f(U_n) = y)) \end{aligned}$$

## Proving Lemma 9

The lemma follows by the next claim:

### Claim 10

$SD((f(U_n), H, H(U_n)), (f(U_n), H, U_1)) = \text{neg}(n)$ , where  $H = H_n$  is uniformly distributed over  $\mathcal{H}_n$ .

Proving the claim. For  $y \in f(\{0, 1\}^n)$ , let  $X_y$  be uniformly distributed over  $f^{-1}(y) := \{x \in \{0, 1\}^n : f(x) = y\}$ . Compute

$$\begin{aligned} &SD((f(U_n), H, H(U_n)), (f(U_n), H, U_1)) \\ &= \sum_{y \in f(\{0, 1\}^n)} \Pr[f(U_n) = y] \cdot \\ &\quad SD((f(U_n), H, H(U_n) \mid f(U_n) = y), (f(U_n), H, U_1 \mid f(U_n) = y)) \\ &= \sum_{y \in f(\{0, 1\}^n)} \Pr[f(U_n) = y] \cdot SD((y, H, H(X_y)), (y, H, U_1)) \end{aligned}$$

## Proving Lemma 9

The lemma follows by the next claim:

### Claim 10

$SD((f(U_n), H, H(U_n)), (f(U_n), H, U_1)) = \text{neg}(n)$ , where  $H = H_n$  is uniformly distributed over  $\mathcal{H}_n$ .

Proving the claim. For  $y \in f(\{0, 1\}^n)$ , let  $X_y$  be uniformly distributed over  $f^{-1}(y) := \{x \in \{0, 1\}^n : f(x) = y\}$ . Compute

$$\begin{aligned} & SD((f(U_n), H, H(U_n)), (f(U_n), H, U_1)) \\ &= \sum_{y \in f(\{0, 1\}^n)} \Pr[f(U_n) = y] \cdot \\ & \quad SD((f(U_n), H, H(U_n) \mid f(U_n) = y), (f(U_n), H, U_1 \mid f(U_n) = y)) \\ &= \sum_{y \in f(\{0, 1\}^n)} \Pr[f(U_n) = y] \cdot SD((y, H, H(X_y)), (y, H, U_1)) \\ &\leq \max_{y \in f(\{0, 1\}^n)} SD((y, H, H(X_y)), (y, H, U_1)) \end{aligned}$$



## Proving Lemma 9

The lemma follows by the next claim:

### Claim 10

$SD((f(U_n), H, H(U_n)), (f(U_n), H, U_1)) = \text{neg}(n)$ , where  $H = H_n$  is uniformly distributed over  $\mathcal{H}_n$ .

Proving the claim. For  $y \in f(\{0, 1\}^n)$ , let  $X_y$  be uniformly distributed over  $f^{-1}(y) := \{x \in \{0, 1\}^n : f(x) = y\}$ . Compute

$$\begin{aligned} & SD((f(U_n), H, H(U_n)), (f(U_n), H, U_1)) \\ &= \sum_{y \in f(\{0, 1\}^n)} \Pr[f(U_n) = y] \cdot \\ & \quad SD((f(U_n), H, H(U_n) \mid f(U_n) = y), (f(U_n), H, U_1 \mid f(U_n) = y)) \\ &= \sum_{y \in f(\{0, 1\}^n)} \Pr[f(U_n) = y] \cdot SD((y, H, H(X_y)), (y, H, U_1)) \\ &\leq \max_{y \in f(\{0, 1\}^n)} SD((y, H, H(X_y)), (y, H, U_1)) \\ &= \max_{y \in f(\{0, 1\}^n)} SD((H, H(X_y)), (H, U_1)) \end{aligned}$$

## Proving Lemma 9, cont.

Since  $H_\infty(X_y) = \log(d(n))$  for any  $y \in f(\{0, 1\}^n)$ ,

## Proving Lemma 9, cont.

Since  $H_\infty(X_y) = \log(d(n))$  for any  $y \in f(\{0, 1\}^n)$ , the leftover hash lemma (Lemma 6) yields that

$$\begin{aligned} \text{SD}((H, H(X_y)), (H, U_1)) &\leq 2^{(1-H_\infty(X_y)-2)/2} \\ &= 2^{(1-\log(d(n)))/2} = \text{neg}(n). \quad \square \end{aligned}$$

## Section 2

# Proving GL – The Computational Case

# Proving Goldreich-Levin Theorem

## Theorem 11 (Goldreich-Levin)

For  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$ , define  $g: \{0, 1\}^n \times \{0, 1\}^n \mapsto \{0, 1\}^n \times \{0, 1\}^n$  as  $g(x, r) = (f(x), r)$ .

If  $f$  is one-way, then  $b(x, r) := \langle x, r \rangle_2$  is an hardcore predicate of  $g$ .

## Proving Goldreich-Levin Theorem

### Theorem 11 (Goldreich-Levin)

For  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$ , define  $g: \{0, 1\}^n \times \{0, 1\}^n \mapsto \{0, 1\}^n \times \{0, 1\}^n$  as  $g(x, r) = (f(x), r)$ .

If  $f$  is one-way, then  $b(x, r) := \langle x, r \rangle_2$  is an hardcore predicate of  $g$ .

Proof: Assume  $\exists$  PPT  $A$ ,  $p \in \text{poly}$  and infinite set  $\mathcal{I} \subseteq \mathbb{N}$  with

$$\Pr[A(g(U_n, R_n)) = b(U_n, R_n)] \geq \frac{1}{2} + \frac{1}{p(n)}, \quad (1)$$

for any  $n \in \mathcal{I}$ , where  $U_n$  and  $R_n$  are uniformly (and independently) distributed over  $\{0, 1\}^n$ .

# Proving Goldreich-Levin Theorem

## Theorem 11 (Goldreich-Levin)

For  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$ , define  $g: \{0, 1\}^n \times \{0, 1\}^n \mapsto \{0, 1\}^n \times \{0, 1\}^n$  as  $g(x, r) = (f(x), r)$ .

If  $f$  is one-way, then  $b(x, r) := \langle x, r \rangle_2$  is an hardcore predicate of  $g$ .

Proof: Assume  $\exists$  PPT  $A$ ,  $p \in \text{poly}$  and infinite set  $\mathcal{I} \subseteq \mathbb{N}$  with

$$\Pr[A(g(U_n, R_n)) = b(U_n, R_n)] \geq \frac{1}{2} + \frac{1}{p(n)}, \quad (1)$$

for any  $n \in \mathcal{I}$ , where  $U_n$  and  $R_n$  are uniformly (and independently) distributed over  $\{0, 1\}^n$ .

We show  $\exists$  PPT  $B$  and  $q \in \text{poly}$  with

$$\Pr_{y \leftarrow f(U_n)}[B(y) \in f^{-1}(y)] \geq \frac{1}{q(n)}, \quad (2)$$

for every  $n \in \mathcal{I}$ .

# Proving Goldreich-Levin Theorem

## Theorem 11 (Goldreich-Levin)

For  $f: \{0, 1\}^n \mapsto \{0, 1\}^n$ , define  $g: \{0, 1\}^n \times \{0, 1\}^n \mapsto \{0, 1\}^n \times \{0, 1\}^n$  as  $g(x, r) = (f(x), r)$ .

If  $f$  is one-way, then  $b(x, r) := \langle x, r \rangle_2$  is an hardcore predicate of  $g$ .

Proof: Assume  $\exists$  PPT  $A$ ,  $p \in \text{poly}$  and infinite set  $\mathcal{I} \subseteq \mathbb{N}$  with

$$\Pr[A(g(U_n, R_n)) = b(U_n, R_n)] \geq \frac{1}{2} + \frac{1}{p(n)}, \quad (1)$$

for any  $n \in \mathcal{I}$ , where  $U_n$  and  $R_n$  are uniformly (and independently) distributed over  $\{0, 1\}^n$ .

We show  $\exists$  PPT  $B$  and  $q \in \text{poly}$  with

$$\Pr_{y \leftarrow f(U_n)}[B(y) \in f^{-1}(y)] \geq \frac{1}{q(n)}, \quad (2)$$

for every  $n \in \mathcal{I}$ . In the following fix  $n \in \mathcal{I}$ .



## Focusing on a good set

### Claim 12

There exists a set  $\mathcal{S} \subseteq \{0, 1\}^n$  with

- 1  $\frac{|\mathcal{S}|}{2^n} \geq \frac{1}{2p(n)}$ , and
- 2  $\Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{1}{2} + \frac{1}{2p(n)}, \forall x \in \mathcal{S}.$

## Focusing on a good set

### Claim 12

There exists a set  $\mathcal{S} \subseteq \{0, 1\}^n$  with

- 1  $\frac{|\mathcal{S}|}{2^n} \geq \frac{1}{2p(n)}$ , and
- 2  $\Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{1}{2} + \frac{1}{2p(n)}, \forall x \in \mathcal{S}.$

Proof:

## Focusing on a good set

### Claim 12

There exists a set  $\mathcal{S} \subseteq \{0, 1\}^n$  with

- 1  $\frac{|\mathcal{S}|}{2^n} \geq \frac{1}{2p(n)}$ , and
- 2  $\Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{1}{2} + \frac{1}{2p(n)}, \forall x \in \mathcal{S}.$

Proof: Let  $\mathcal{S} := \{x \in \{0, 1\}^n : \Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{1}{2} + \frac{1}{2p(n)}\}.$

## Focusing on a good set

### Claim 12

There exists a set  $\mathcal{S} \subseteq \{0, 1\}^n$  with

- 1  $\frac{|\mathcal{S}|}{2^n} \geq \frac{1}{2p(n)}$ , and
- 2  $\Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{1}{2} + \frac{1}{2p(n)}, \forall x \in \mathcal{S}.$

Proof: Let  $\mathcal{S} := \{x \in \{0, 1\}^n : \Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{1}{2} + \frac{1}{2p(n)}\}.$

$$\Pr[A(g(U_n, R_n)) = b(U_n, R_n)] \leq \Pr[U_n \notin \mathcal{S}] \cdot \left(\frac{1}{2}\right) + \Pr[U_n \in \mathcal{S}] \cdot \left(\frac{1}{2} + \frac{1}{2p(n)}\right)$$

## Focusing on a good set

### Claim 12

There exists a set  $\mathcal{S} \subseteq \{0, 1\}^n$  with

- 1  $\frac{|\mathcal{S}|}{2^n} \geq \frac{1}{2p(n)}$ , and
- 2  $\Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{1}{2} + \frac{1}{2p(n)}, \forall x \in \mathcal{S}.$

Proof: Let  $\mathcal{S} := \{x \in \{0, 1\}^n : \Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{1}{2} + \frac{1}{2p(n)}\}.$

$$\begin{aligned}\Pr[A(g(U_n, R_n)) = b(U_n, R_n)] &\leq \Pr[U_n \notin \mathcal{S}] \cdot \left(\frac{1}{2} + \frac{1}{2p(n)}\right) + \Pr[U_n \in \mathcal{S}] \\ &\leq \left(\frac{1}{2} + \frac{1}{2p(n)}\right) + \Pr[U_n \in \mathcal{S}] \square\end{aligned}$$

## Focusing on a good set

### Claim 12

There exists a set  $\mathcal{S} \subseteq \{0, 1\}^n$  with

- 1  $\frac{|\mathcal{S}|}{2^n} \geq \frac{1}{2p(n)}$ , and
- 2  $\Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{1}{2} + \frac{1}{2p(n)}, \forall x \in \mathcal{S}.$

Proof: Let  $\mathcal{S} := \{x \in \{0, 1\}^n : \Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{1}{2} + \frac{1}{2p(n)}\}.$

$$\begin{aligned}\Pr[A(g(U_n, R_n)) = b(U_n, R_n)] &\leq \Pr[U_n \notin \mathcal{S}] \cdot \left(\frac{1}{2} + \frac{1}{2p(n)}\right) + \Pr[U_n \in \mathcal{S}] \\ &\leq \left(\frac{1}{2} + \frac{1}{2p(n)}\right) + \Pr[U_n \in \mathcal{S}] \square\end{aligned}$$

We conclude the theorem's proof showing exist  $q \in \text{poly}$  and PPT  $B$ :

$$\Pr[B(f(x)) \in f^{-1}(f(x))] \geq \frac{1}{q(n)}, \quad (3)$$

for every  $x \in \mathcal{S}.$

## Focusing on a good set

### Claim 12

There exists a set  $\mathcal{S} \subseteq \{0, 1\}^n$  with

- 1  $\frac{|\mathcal{S}|}{2^n} \geq \frac{1}{2p(n)}$ , and
- 2  $\Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{1}{2} + \frac{1}{2p(n)}, \forall x \in \mathcal{S}.$

Proof: Let  $\mathcal{S} := \{x \in \{0, 1\}^n : \Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{1}{2} + \frac{1}{2p(n)}\}.$

$$\begin{aligned}\Pr[A(g(U_n, R_n)) = b(U_n, R_n)] &\leq \Pr[U_n \notin \mathcal{S}] \cdot \left(\frac{1}{2} + \frac{1}{2p(n)}\right) + \Pr[U_n \in \mathcal{S}] \\ &\leq \left(\frac{1}{2} + \frac{1}{2p(n)}\right) + \Pr[U_n \in \mathcal{S}] \square\end{aligned}$$

We conclude the theorem's proof showing exist  $q \in \text{poly}$  and PPT  $B$ :

$$\Pr[B(f(x)) \in f^{-1}(f(x))] \geq \frac{1}{q(n)}, \quad (3)$$

for every  $x \in \mathcal{S}$ . In the following we fix  $x \in \mathcal{S}$ .

# The Perfect Case

$$\Pr[A(f(x), R_n) = b(x, R_n)] = 1$$



●  $A(f(x), r) = b(x, r)$

●  $A(f(x), r) \neq b(x, r)$



# The Perfect Case

$$\Pr[A(f(x), R_n) = b(x, R_n)] = 1$$



●  $A(f(x), r) = b(x, r)$

●  $A(f(x), r) \neq b(x, r)$

In particular,  $A(f(x), e^i) = b(x, e^i)$  for every  $i \in [n]$ , where  $e^i = (\underbrace{0, \dots, 0}_{i-1}, 1, \underbrace{0, \dots, 0}_{n-i})$ .

# The Perfect Case

$$\Pr[A(f(x), R_n) = b(x, R_n)] = 1$$



●  $A(f(x), r) = b(x, r)$

●  $A(f(x), r) \neq b(x, r)$

In particular,  $A(f(x), e^i) = b(x, e^i)$  for every  $i \in [n]$ , where  $e^i = (\underbrace{0, \dots, 0}_{i-1}, 1, \underbrace{0, \dots, 0}_{n-i})$ .

Hence,  $x_i = \langle x, e^i \rangle_2$

# The Perfect Case

$$\Pr[A(f(x), R_n) = b(x, R_n)] = 1$$



●  $A(f(x), r) = b(x, r)$

●  $A(f(x), r) \neq b(x, r)$

In particular,  $A(f(x), e^i) = b(x, e^i)$  for every  $i \in [n]$ , where  $e^i = (\underbrace{0, \dots, 0}_{i-1}, 1, \underbrace{0, \dots, 0}_{n-i})$ .

Hence,  $x_i = \langle x, e^i \rangle_2 = b(x, e^i) = A(f(x), e^i)$

# The Perfect Case

$$\Pr[A(f(x), R_n) = b(x, R_n)] = 1$$



●  $A(f(x), r) = b(x, r)$

●  $A(f(x), r) \neq b(x, r)$

In particular,  $A(f(x), e^i) = b(x, e^i)$  for every  $i \in [n]$ , where  $e^i = (\underbrace{0, \dots, 0}_{i-1}, 1, \underbrace{0, \dots, 0}_{n-i})$ .

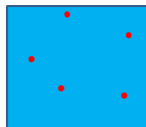
Hence,  $x_i = \langle x, e^i \rangle_2 = b(x, e^i) = A(f(x), e^i)$

## Algorithm 13 (Inverter B on input $y$ )

Return  $(A(y, e^1), \dots, A(y, e^n))$ .

## Easy case

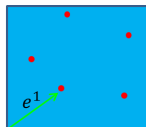
$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq 1 - \text{neg}(n)$$



- $A(f(x), r) = b(x, r)$
- $A(f(x), r) \neq b(x, r)$

## Easy case

$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq 1 - \text{neg}(n)$$

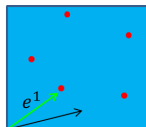


●  $A(f(x), r) = b(x, r)$

●  $A(f(x), r) \neq b(x, r)$

## Easy case

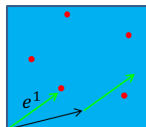
$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq 1 - \text{neg}(n)$$



- $A(f(x), r) = b(x, r)$
- $A(f(x), r) \neq b(x, r)$

## Easy case

$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq 1 - \text{neg}(n)$$

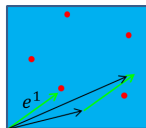


- $A(f(x), r) = b(x, r)$
- $A(f(x), r) \neq b(x, r)$



## Easy case

$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq 1 - \text{neg}(n)$$

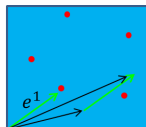


●  $A(f(x), r) = b(x, r)$

●  $A(f(x), r) \neq b(x, r)$

## Easy case

$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq 1 - \text{neg}(n)$$



●  $A(f(x), r) = b(x, r)$

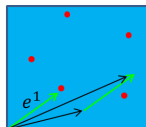
●  $A(f(x), r) \neq b(x, r)$

### Fact 14

①  $b(x, w) \oplus b(x, y) = b(x, w \oplus y)$  for every  $w, w, y \in \{0, 1\}^n$ .

## Easy case

$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq 1 - \text{neg}(n)$$



●  $A(f(x), r) = b(x, r)$

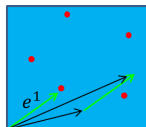
●  $A(f(x), r) \neq b(x, r)$

### Fact 14

- 1  $b(x, w) \oplus b(x, y) = b(x, w \oplus y)$  for every  $w, y \in \{0, 1\}^n$ .
- 2  $\forall r \in \{0, 1\}^n$ , the rv  $(R_n \oplus r)$  is uniformly distributed over  $\{0, 1\}^n$ .

## Easy case

$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq 1 - \text{neg}(n)$$



- $A(f(x), r) = b(x, r)$
- $A(f(x), r) \neq b(x, r)$

### Fact 14

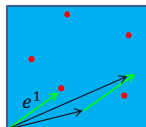
- 1  $b(x, w) \oplus b(x, y) = b(x, w \oplus y)$  for every  $w, y \in \{0, 1\}^n$ .
- 2  $\forall r \in \{0, 1\}^n$ , the rv  $(R_n \oplus r)$  is uniformly distributed over  $\{0, 1\}^n$ .

Hence,  $\forall i \in [n]$ :

- 1  $x_i = b(x, e^i) = b(x, r) \oplus b(x, r \oplus e^i)$  for every  $r \in \{0, 1\}^n$

## Easy case

$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq 1 - \text{neg}(n)$$



- $A(f(x), r) = b(x, r)$
- $A(f(x), r) \neq b(x, r)$

### Fact 14

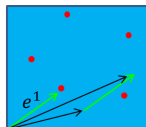
- 1  $b(x, w) \oplus b(x, y) = b(x, w \oplus y)$  for every  $w, y \in \{0, 1\}^n$ .
- 2  $\forall r \in \{0, 1\}^n$ , the rv  $(R_n \oplus r)$  is uniformly distributed over  $\{0, 1\}^n$ .

Hence,  $\forall i \in [n]$ :

- 1  $x_i = b(x, e^i) = b(x, r) \oplus b(x, r \oplus e^i)$  for every  $r \in \{0, 1\}^n$
- 2  $\Pr[A(f(x), R_n) = b(x, R_n) \wedge A(f(x), R_n \oplus e^i) = b(x, R_n \oplus e^i)] \geq 1 - \text{neg}(n)$

## Easy case

$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq 1 - \text{neg}(n)$$



- $A(f(x), r) = b(x, r)$
- $A(f(x), r) \neq b(x, r)$

### Fact 14

- 1  $b(x, w) \oplus b(x, y) = b(x, w \oplus y)$  for every  $w, y \in \{0, 1\}^n$ .
- 2  $\forall r \in \{0, 1\}^n$ , the rv  $(R_n \oplus r)$  is uniformly distributed over  $\{0, 1\}^n$ .

Hence,  $\forall i \in [n]$ :

- 1  $x_i = b(x, e^i) = b(x, r) \oplus b(x, r \oplus e^i)$  for every  $r \in \{0, 1\}^n$
- 2  $\Pr[A(f(x), R_n) = b(x, R_n) \wedge A(f(x), R_n \oplus e^i) = b(x, R_n \oplus e^i)] \geq 1 - \text{neg}(n)$

### Algorithm 15 (Inverter B on input $y$ )

Return  $(A(y, R_n) \oplus A(y, R_n \oplus e^1), \dots, A(y, R_n) \oplus A(y, R_n \oplus e^n))$ .

## Proving Fact 14

① For  $w, w, y \in \{0, 1\}^n$ :

$$\begin{aligned} b(x, y) \oplus b(x, w) &= \left( \bigoplus_{i=1}^n x_i \cdot y_i \right) \oplus \left( \bigoplus_{i=1}^n x_i \cdot w_i \right) \\ &= \bigoplus_{i=1}^n x_i \cdot (y_i \oplus w_i) \\ &= b(x, y \oplus w) \end{aligned}$$

## Proving Fact 14

1 For  $w, w, y \in \{0, 1\}^n$ :

$$\begin{aligned} b(x, y) \oplus b(x, w) &= \left( \bigoplus_{i=1}^n x_i \cdot y_i \right) \oplus \left( \bigoplus_{i=1}^n x_i \cdot w_i \right) \\ &= \bigoplus_{i=1}^n x_i \cdot (y_i \oplus w_i) \\ &= b(x, y \oplus w) \end{aligned}$$

2 For  $r, y \in \{0, 1\}^n$ :

$$\Pr[R_n \oplus r = y] = \Pr[R_n = y \oplus r] = 2^{-n}$$



## Intermediate Case

$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{3}{4} + \frac{1}{q(n)}$$



- $A(f(x), r) = b(x, r)$
- $A(f(x), r) \neq b(x, r)$

## Intermediate Case

$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{3}{4} + \frac{1}{q(n)}$$

For any  $i \in [n]$

$$\begin{aligned} & \Pr[A(f(x), R_n) \oplus A(f(x), R_n \oplus e^i) = x_i] \\ & \geq \Pr[A(f(x), R_n) = b(x, R_n) \wedge A(f(x), R_n \oplus e^i) = b(x, R_n \oplus e^i)] \end{aligned}$$



●  $A(f(x), r) = b(x, r)$

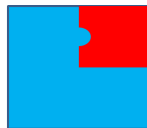
●  $A(f(x), r) \neq b(x, r)$

## Intermediate Case

$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{3}{4} + \frac{1}{q(n)}$$

For any  $i \in [n]$

$$\begin{aligned} & \Pr[A(f(x), R_n) \oplus A(f(x), R_n \oplus e^i) = x_i] \\ & \geq \Pr[A(f(x), R_n) = b(x, R_n) \wedge A(f(x), R_n \oplus e^i) = b(x, R_n \oplus e^i)] \\ & \geq 1 - \left(1 - \left(\frac{3}{4} + \frac{1}{q(n)}\right)\right) - \left(1 - \left(\frac{3}{4} + \frac{1}{q(n)}\right)\right) \end{aligned}$$



- $A(f(x), r) = b(x, r)$
- $A(f(x), r) \neq b(x, r)$

## Intermediate Case

$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{3}{4} + \frac{1}{q(n)}$$

For any  $i \in [n]$

$$\begin{aligned} & \Pr[A(f(x), R_n) \oplus A(f(x), R_n \oplus e^i) = x_i] \\ & \geq \Pr[A(f(x), R_n) = b(x, R_n) \wedge A(f(x), R_n \oplus e^i) = b(x, R_n \oplus e^i)] \\ & \geq 1 - \left(1 - \left(\frac{3}{4} + \frac{1}{q(n)}\right)\right) - \left(1 - \left(\frac{3}{4} + \frac{1}{q(n)}\right)\right) = \frac{1}{2} + \frac{2}{q(n)} \end{aligned}$$



- $A(f(x), r) = b(x, r)$
- $A(f(x), r) \neq b(x, r)$

## Intermediate Case

$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{3}{4} + \frac{1}{q(n)}$$

For any  $i \in [n]$

$$\begin{aligned} & \Pr[A(f(x), R_n) \oplus A(f(x), R_n \oplus e^i) = x_i] \\ & \geq \Pr[A(f(x), R_n) = b(x, R_n) \wedge A(f(x), R_n \oplus e^i) = b(x, R_n \oplus e^i)] \\ & \geq 1 - \left(1 - \left(\frac{3}{4} + \frac{1}{q(n)}\right)\right) - \left(1 - \left(\frac{3}{4} + \frac{1}{q(n)}\right)\right) = \frac{1}{2} + \frac{2}{q(n)} \end{aligned}$$



- $A(f(x), r) = b(x, r)$
- $A(f(x), r) \neq b(x, r)$

### Algorithm 16 (Inverter B on input $y \in \{0, 1\}^n$ )

- 1 For every  $i \in [n]$ 
  - 1 Sample  $r^1, \dots, r^v \in \{0, 1\}^n$  uniformly at random
  - 2 Let  $m_i = \text{maj}_{j \in [v]} \{(A(y, r^j) \oplus A(y, r^j \oplus e^i))\}$
- 2 Output  $(m_1, \dots, m_n)$

## B's Success Provability

The following claim holds for “large enough”  $v = v(n) \in \text{poly}(n)$ .

## B's Success Provability

The following claim holds for “large enough”  $v = v(n) \in \text{poly}(n)$ .

### Claim 17

For every  $i \in [n]$ , it holds that  $\Pr[m_i = x_i] \geq 1 - \text{neg}(n)$ .

## B's Success Provability

The following claim holds for “large enough”  $v = v(n) \in \text{poly}(n)$ .

### Claim 17

For every  $i \in [n]$ , it holds that  $\Pr[m_i = x_i] \geq 1 - \text{neg}(n)$ .

Proof: For  $j \in [v]$ , let the indicator rv  $W^j$  be 1, iff  $A(f(x), r^j) \oplus A(f(x), r^j \oplus e^j) = x_i$ .



## B's Success Provability

The following claim holds for “large enough”  $v = v(n) \in \text{poly}(n)$ .

### Claim 17

For every  $i \in [n]$ , it holds that  $\Pr[m_i = x_i] \geq 1 - \text{neg}(n)$ .

Proof: For  $j \in [v]$ , let the indicator rv  $W^j$  be 1, iff  $A(f(x), r^j) \oplus A(f(x), r^j \oplus e^j) = x_i$ .

We want to lowerbound  $\Pr \left[ \sum_{j=1}^v W^j > \frac{v}{2} \right]$ .

## B's Success Provability

The following claim holds for “large enough”  $v = v(n) \in \text{poly}(n)$ .

### Claim 17

For every  $i \in [n]$ , it holds that  $\Pr[m_i = x_i] \geq 1 - \text{neg}(n)$ .

Proof: For  $j \in [v]$ , let the indicator rv  $W^j$  be 1, iff  $A(f(x), r^j) \oplus A(f(x), r^j \oplus e^j) = x_i$ .

We want to lowerbound  $\Pr \left[ \sum_{j=1}^v W^j > \frac{v}{2} \right]$ .

- The  $W^j$  are iids and  $E[W^j] \geq \frac{1}{2} + \frac{2}{q(n)}$  for every  $j \in [v]$

## B's Success Provability

The following claim holds for “large enough”  $v = v(n) \in \text{poly}(n)$ .

### Claim 17

For every  $i \in [n]$ , it holds that  $\Pr[m_i = x_i] \geq 1 - \text{neg}(n)$ .

Proof: For  $j \in [v]$ , let the indicator rv  $W^j$  be 1, iff  $A(f(x), r^j) \oplus A(f(x), r^j \oplus e^j) = x_i$ .

We want to lowerbound  $\Pr\left[\sum_{j=1}^v W^j > \frac{v}{2}\right]$ .

- The  $W^j$  are iids and  $E[W^j] \geq \frac{1}{2} + \frac{2}{q(n)}$  for every  $j \in [v]$

### Lemma 18 (Hoeffding's inequality)

Let  $X^1, \dots, X^v$  be iids over  $[0, 1]$  with expectation  $\mu$ . Then,

$\Pr\left[\left|\frac{\sum_{j=1}^v X^j}{v} - \mu\right| \geq \varepsilon\right] \leq 2 \cdot \exp(-2\varepsilon^2 v)$  for every  $\varepsilon > 0$ .

## B's Success Provability

The following claim holds for “large enough”  $v = v(n) \in \text{poly}(n)$ .

### Claim 17

For every  $i \in [n]$ , it holds that  $\Pr[m_i = x_i] \geq 1 - \text{neg}(n)$ .

Proof: For  $j \in [v]$ , let the indicator rv  $W^j$  be 1, iff  $A(f(x), r^j) \oplus A(f(x), r^j \oplus e^j) = x_i$ .

We want to lowerbound  $\Pr \left[ \sum_{j=1}^v W^j > \frac{v}{2} \right]$ .

- The  $W^j$  are iids and  $E[W^j] \geq \frac{1}{2} + \frac{2}{q(n)}$  for every  $j \in [v]$

### Lemma 18 (Hoeffding's inequality)

Let  $X^1, \dots, X^v$  be iids over  $[0, 1]$  with expectation  $\mu$ . Then,  
 $\Pr \left[ \left| \frac{\sum_{j=1}^v X^j}{v} - \mu \right| \geq \varepsilon \right] \leq 2 \cdot \exp(-2\varepsilon^2 v)$  for every  $\varepsilon > 0$ .

We complete the proof taking  $X^j = W^j$ ,  $\varepsilon = 1/4q(n)$  and  $v \in \omega(\log(n) \cdot q(n)^2)$ .

## The actual (hard) case

$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{1}{2} + \frac{1}{q(n)}$$



- $A(f(x), r) = b(x, r)$
- $A(f(x), r) \neq b(x, r)$

## The actual (hard) case

$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{1}{2} + \frac{1}{q(n)}$$



- $A(f(x), r) = b(x, r)$
- $A(f(x), r) \neq b(x, r)$

- What goes wrong?

## The actual (hard) case

$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{1}{2} + \frac{1}{q(n)}$$



- $A(f(x), r) = b(x, r)$
- $A(f(x), r) \neq b(x, r)$

- What goes wrong?

$$\Pr[A(f(x), R_n) \oplus A(f(x), R_n \oplus e^i) = x_i] \geq \frac{2}{q(n)}$$

## The actual (hard) case

$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{1}{2} + \frac{1}{q(n)}$$



- $A(f(x), r) = b(x, r)$
- $A(f(x), r) \neq b(x, r)$

- What goes wrong?

$$\Pr[A(f(x), R_n) \oplus A(f(x), R_n \oplus e^i) = x_i] \geq \frac{2}{q(n)}$$

- Hence, using a random guess does better than using **A** :-<



## The actual (hard) case

$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{1}{2} + \frac{1}{q(n)}$$



- $A(f(x), r) = b(x, r)$
- $A(f(x), r) \neq b(x, r)$

- What goes wrong?

$$\Pr[A(f(x), R_n) \oplus A(f(x), R_n \oplus e^i) = x_i] \geq \frac{2}{q(n)}$$

- Hence, using a random guess does better than using  $A$  :-<
- Idea: guess the values of  $\{b(x, r^1), \dots, b(x, r^v)\}$   
(instead of calling  $\{A(f(x), r^1), \dots, A(f(x), r^v)\}$ )

## The actual (hard) case

$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{1}{2} + \frac{1}{q(n)}$$



- $A(f(x), r) = b(x, r)$
- $A(f(x), r) \neq b(x, r)$

- What goes wrong?

$$\Pr[A(f(x), R_n) \oplus A(f(x), R_n \oplus e^i) = x_i] \geq \frac{2}{q(n)}$$

- Hence, using a random guess does better than using  $A$  :-<
- Idea: guess the values of  $\{b(x, r^1), \dots, b(x, r^v)\}$   
(instead of calling  $\{A(f(x), r^1), \dots, A(f(x), r^v)\}$ )

**Problem:** negligible success probability

## The actual (hard) case

$$\Pr[A(f(x), R_n) = b(x, R_n)] \geq \frac{1}{2} + \frac{1}{q(n)}$$



- $A(f(x), r) = b(x, r)$
- $A(f(x), r) \neq b(x, r)$

- What goes wrong?

$$\Pr[A(f(x), R_n) \oplus A(f(x), R_n \oplus e^i) = x_i] \geq \frac{2}{q(n)}$$

- Hence, using a random guess does better than using  $A$  :-<
- Idea: guess the values of  $\{b(x, r^1), \dots, b(x, r^v)\}$   
(instead of calling  $\{A(f(x), r^1), \dots, A(f(x), r^v)\}$ )

**Problem:** negligible success probability

**Solution:** choose the samples in a **correlated** manner

## Algorithm B

- Fix  $\ell = \ell(n)$  (will be  $O(\log n)$ ) and set  $v = 2^\ell - 1$ .

## Algorithm B

- Fix  $\ell = \ell(n)$  (will be  $O(\log n)$ ) and set  $v = 2^\ell - 1$ .

## Algorithm B

- Fix  $\ell = \ell(n)$  (will be  $O(\log n)$ ) and set  $v = 2^\ell - 1$ .
- In the following  $\mathcal{L} \subseteq [\ell]$  stands for a **non empty** choice

## Algorithm B

- Fix  $\ell = \ell(n)$  (will be  $O(\log n)$ ) and set  $v = 2^\ell - 1$ .
- In the following  $\mathcal{L} \subseteq [\ell]$  stands for a **non empty** choice

## Algorithm B

- Fix  $\ell = \ell(n)$  (will be  $O(\log n)$ ) and set  $v = 2^\ell - 1$ .
- In the following  $\mathcal{L} \subseteq [\ell]$  stands for a **non empty** choice

### Algorithm 19 (Inverter B on $y = f(x) \in \{0, 1\}^n$ )

- 1 Sample uniformly (and independently)  $t^1, \dots, t^\ell \in \{0, 1\}^n$
- 2 Guess the value of  $\{b(x, t^i)\}_{i \in [\ell]}$
- 3 For all  $\mathcal{L} \subseteq [\ell]$ : set  $r^\mathcal{L} = \bigoplus_{i \in \mathcal{L}} t^i$  and compute  $b(x, r^\mathcal{L}) = \bigoplus_{i \in \mathcal{L}} b(x, t^i)$ .
- 4 For all  $i \in [n]$ , let  $m_i = \text{maj}_{\mathcal{L} \subseteq [\ell]} \{A(f(x), r^\mathcal{L} \oplus e^i) \oplus b(x, r^\mathcal{L})\}$
- 5 Output  $(m_1, \dots, m_n)$



## Algorithm B

- Fix  $\ell = \ell(n)$  (will be  $O(\log n)$ ) and set  $v = 2^\ell - 1$ .
- In the following  $\mathcal{L} \subseteq [\ell]$  stands for a **non empty** choice

### Algorithm 19 (Inverter B on $y = f(x) \in \{0, 1\}^n$ )

- 1 Sample uniformly (and independently)  $t^1, \dots, t^\ell \in \{0, 1\}^n$
- 2 Guess the value of  $\{b(x, t^i)\}_{i \in [\ell]}$
- 3 For all  $\mathcal{L} \subseteq [\ell]$ : set  $r^\mathcal{L} = \bigoplus_{i \in \mathcal{L}} t^i$  and compute  $b(x, r^\mathcal{L}) = \bigoplus_{i \in \mathcal{L}} b(x, t^i)$ .
- 4 For all  $i \in [n]$ , let  $m_i = \text{maj}_{\mathcal{L} \subseteq [\ell]} \{A(f(x), r^\mathcal{L} \oplus e^i) \oplus b(x, r^\mathcal{L})\}$
- 5 Output  $(m_1, \dots, m_n)$

- Fix  $i \in [n]$ , and let  $W^\mathcal{L}$  be 1 iff  $A(f(x), r^\mathcal{L} \oplus e^i) \oplus b(x, r^\mathcal{L}) = x_i$ .

## Algorithm B

- Fix  $\ell = \ell(n)$  (will be  $O(\log n)$ ) and set  $v = 2^\ell - 1$ .
- In the following  $\mathcal{L} \subseteq [\ell]$  stands for a **non empty** choice

### Algorithm 19 (Inverter B on $y = f(x) \in \{0, 1\}^n$ )

- 1 Sample uniformly (and independently)  $t^1, \dots, t^\ell \in \{0, 1\}^n$
- 2 Guess the value of  $\{b(x, t^i)\}_{i \in [\ell]}$
- 3 For all  $\mathcal{L} \subseteq [\ell]$ : set  $r^\mathcal{L} = \bigoplus_{i \in \mathcal{L}} t^i$  and compute  $b(x, r^\mathcal{L}) = \bigoplus_{i \in \mathcal{L}} b(x, t^i)$ .
- 4 For all  $i \in [n]$ , let  $m_i = \text{maj}_{\mathcal{L} \subseteq [\ell]} \{A(f(x), r^\mathcal{L} \oplus e^i) \oplus b(x, r^\mathcal{L})\}$
- 5 Output  $(m_1, \dots, m_n)$

- Fix  $i \in [n]$ , and let  $W^\mathcal{L}$  be 1 iff  $A(f(x), r^\mathcal{L} \oplus e^i) \oplus b(x, r^\mathcal{L}) = x_i$ .
- We want to lowerbound  $\Pr \left[ \sum_{\mathcal{L} \subseteq [\ell]} W^\mathcal{L} > \frac{v}{2} \right]$

## Algorithm B

- Fix  $\ell = \ell(n)$  (will be  $O(\log n)$ ) and set  $v = 2^\ell - 1$ .
- In the following  $\mathcal{L} \subseteq [\ell]$  stands for a **non empty** choice

### Algorithm 19 (Inverter B on $y = f(x) \in \{0, 1\}^n$ )

- 1 Sample uniformly (and independently)  $t^1, \dots, t^\ell \in \{0, 1\}^n$
- 2 Guess the value of  $\{b(x, t^i)\}_{i \in [\ell]}$
- 3 For all  $\mathcal{L} \subseteq [\ell]$ : set  $r^\mathcal{L} = \bigoplus_{i \in \mathcal{L}} t^i$  and compute  $b(x, r^\mathcal{L}) = \bigoplus_{i \in \mathcal{L}} b(x, t^i)$ .
- 4 For all  $i \in [n]$ , let  $m_i = \text{maj}_{\mathcal{L} \subseteq [\ell]} \{A(f(x), r^\mathcal{L} \oplus e^i) \oplus b(x, r^\mathcal{L})\}$
- 5 Output  $(m_1, \dots, m_n)$

- Fix  $i \in [n]$ , and let  $W^\mathcal{L}$  be 1 iff  $A(f(x), r^\mathcal{L} \oplus e^i) \oplus b(x, r^\mathcal{L}) = x_i$ .
- We want to lowerbound  $\Pr \left[ \sum_{\mathcal{L} \subseteq [\ell]} W^\mathcal{L} > \frac{v}{2} \right]$
- Problem: the  $W^\mathcal{L}$ 's are **dependent**!

## Analyzing B's success probability

- 1 Let  $T^1, \dots, T^\ell$  be iid and uniform over  $\{0, 1\}^n$ .
- 2 For  $\mathcal{L} \subseteq [\ell]$ , let  $R^\mathcal{L} = \bigoplus_{i \in \mathcal{L}} T^i$ .

## Analyzing B's success probability

- 1 Let  $T^1, \dots, T^\ell$  be iid and uniform over  $\{0, 1\}^n$ .
- 2 For  $\mathcal{L} \subseteq [\ell]$ , let  $R^\mathcal{L} = \bigoplus_{i \in \mathcal{L}} T^i$ .

### Claim 20

- 1  $\forall \mathcal{L} \subseteq [\ell]$ ,  $R^\mathcal{L}$  is uniformly distributed over  $\{0, 1\}^n$ .
- 2  $\forall w, w' \in \{0, 1\}^n$  and  $\mathcal{L} \neq \mathcal{L}' \subseteq [\ell]$ , it holds that  $\Pr[R^\mathcal{L} = w \wedge R^{\mathcal{L}'} = w'] = \Pr[R^\mathcal{L} = w] \cdot \Pr[R^{\mathcal{L}'} = w'] = 2^{-2n}$ .

## Analyzing B's success probability

- 1 Let  $T^1, \dots, T^\ell$  be iid and uniform over  $\{0, 1\}^n$ .
- 2 For  $\mathcal{L} \subseteq [\ell]$ , let  $R^\mathcal{L} = \bigoplus_{i \in \mathcal{L}} T^i$ .

### Claim 20

- 1  $\forall \mathcal{L} \subseteq [\ell]$ ,  $R^\mathcal{L}$  is uniformly distributed over  $\{0, 1\}^n$ .
- 2  $\forall w, w' \in \{0, 1\}^n$  and  $\mathcal{L} \neq \mathcal{L}' \subseteq [\ell]$ , it holds that  $\Pr[R^\mathcal{L} = w \wedge R^{\mathcal{L}'} = w'] = \Pr[R^\mathcal{L} = w] \cdot \Pr[R^{\mathcal{L}'} = w'] = 2^{-2n}$ .

Proof:

## Analyzing B's success probability

- 1 Let  $T^1, \dots, T^\ell$  be iid and uniform over  $\{0, 1\}^n$ .
- 2 For  $\mathcal{L} \subseteq [\ell]$ , let  $R^\mathcal{L} = \bigoplus_{i \in \mathcal{L}} T^i$ .

### Claim 20

- 1  $\forall \mathcal{L} \subseteq [\ell]$ ,  $R^\mathcal{L}$  is uniformly distributed over  $\{0, 1\}^n$ .
- 2  $\forall w, w' \in \{0, 1\}^n$  and  $\mathcal{L} \neq \mathcal{L}' \subseteq [\ell]$ , it holds that  $\Pr[R^\mathcal{L} = w \wedge R^{\mathcal{L}'} = w'] = \Pr[R^\mathcal{L} = w] \cdot \Pr[R^{\mathcal{L}'} = w'] = 2^{-2n}$ .

Proof: (1) is clear,

## Analyzing B's success probability

- 1 Let  $T^1, \dots, T^\ell$  be iid and uniform over  $\{0, 1\}^n$ .
- 2 For  $\mathcal{L} \subseteq [\ell]$ , let  $R^\mathcal{L} = \bigoplus_{i \in \mathcal{L}} T^i$ .

### Claim 20

- 1  $\forall \mathcal{L} \subseteq [\ell]$ ,  $R^\mathcal{L}$  is uniformly distributed over  $\{0, 1\}^n$ .
- 2  $\forall w, w' \in \{0, 1\}^n$  and  $\mathcal{L} \neq \mathcal{L}' \subseteq [\ell]$ , it holds that  
$$\Pr[R^\mathcal{L} = w \wedge R^{\mathcal{L}'} = w'] = \Pr[R^\mathcal{L} = w] \cdot \Pr[R^{\mathcal{L}'} = w'] = 2^{-2n}.$$

Proof: (1) is clear, we prove (2) in the next slide.



## Proving **Fact 20(2)**

Assume wlg. that  $1 \in (\mathcal{L}' \setminus \mathcal{L})$ .

## Proving Fact 20(2)

Assume wlg. that  $1 \in (\mathcal{L}' \setminus \mathcal{L})$ .

$$\begin{aligned} & \Pr[R^{\mathcal{L}} = w \wedge R^{\mathcal{L}'} = w'] \\ &= \sum_{(t^2, \dots, t^\ell) \in \{0,1\}^{(\ell-1)n}} \Pr[(T^2, \dots, T^\ell) = (t^2, \dots, t^\ell)] \cdot \\ & \quad \Pr[R^{\mathcal{L}} = w \wedge R^{\mathcal{L}'} = w' \mid (T^2, \dots, T^\ell) = (t^2, \dots, t^\ell)] \end{aligned}$$

## Proving Fact 20(2)

Assume wlg. that  $1 \in (\mathcal{L}' \setminus \mathcal{L})$ .

$$\begin{aligned} & \Pr[R^{\mathcal{L}} = w \wedge R^{\mathcal{L}'} = w'] \\ &= \sum_{(t^2, \dots, t^\ell) \in \{0,1\}^{(\ell-1)n}} \Pr[(T^2, \dots, T^\ell) = (t^2, \dots, t^\ell)] \cdot \\ & \quad \Pr[R^{\mathcal{L}} = w \wedge R^{\mathcal{L}'} = w' \mid (T^2, \dots, T^\ell) = (t^2, \dots, t^\ell)] \\ &= \sum_{(t^2, \dots, t^\ell): (\oplus_{i \in \mathcal{L}} t^i) = w} \Pr[(T^2, \dots, T^\ell) = (t^2, \dots, t^\ell)] \\ & \quad \cdot \Pr[R^{\mathcal{L}'} = w' \mid (T^2, \dots, T^\ell) = (t^2, \dots, t^\ell)] \end{aligned}$$

## Proving Fact 20(2)

Assume wlg. that  $1 \in (\mathcal{L}' \setminus \mathcal{L})$ .

$$\begin{aligned} & \Pr[R^{\mathcal{L}} = w \wedge R^{\mathcal{L}'} = w'] \\ &= \sum_{(t^2, \dots, t^\ell) \in \{0,1\}^{(\ell-1)n}} \Pr[(T^2, \dots, T^\ell) = (t^2, \dots, t^\ell)] \cdot \\ & \quad \Pr[R^{\mathcal{L}} = w \wedge R^{\mathcal{L}'} = w' \mid (T^2, \dots, T^\ell) = (t^2, \dots, t^\ell)] \\ &= \sum_{(t^2, \dots, t^\ell): (\oplus_{i \in \mathcal{L}} t^i) = w} \Pr[(T^2, \dots, T^\ell) = (t^2, \dots, t^\ell)] \\ & \quad \cdot \Pr[R^{\mathcal{L}'} = w' \mid (T^2, \dots, T^\ell) = (t^2, \dots, t^\ell)] \\ &= \sum_{(t^2, \dots, t^\ell): (\oplus_{i \in \mathcal{L}} t^i) = w} \Pr[(T^2, \dots, T^\ell) = (t^2, \dots, t^\ell)] \cdot 2^{-n} \end{aligned}$$

## Proving Fact 20(2)

Assume wlg. that  $1 \in (\mathcal{L}' \setminus \mathcal{L})$ .

$$\begin{aligned} & \Pr[R^{\mathcal{L}} = w \wedge R^{\mathcal{L}'} = w'] \\ &= \sum_{(t^2, \dots, t^\ell) \in \{0,1\}^{(\ell-1)n}} \Pr[(T^2, \dots, T^\ell) = (t^2, \dots, t^\ell)] \cdot \\ & \quad \Pr[R^{\mathcal{L}} = w \wedge R^{\mathcal{L}'} = w' \mid (T^2, \dots, T^\ell) = (t^2, \dots, t^\ell)] \\ &= \sum_{(t^2, \dots, t^\ell): (\oplus_{i \in \mathcal{L}} t^i) = w} \Pr[(T^2, \dots, T^\ell) = (t^2, \dots, t^\ell)] \\ & \quad \cdot \Pr[R^{\mathcal{L}'} = w' \mid (T^2, \dots, T^\ell) = (t^2, \dots, t^\ell)] \\ &= \sum_{(t^2, \dots, t^\ell): (\oplus_{i \in \mathcal{L}} t^i) = w} \Pr[(T^2, \dots, T^\ell) = (t^2, \dots, t^\ell)] \cdot 2^{-n} \\ &= 2^{-n} \cdot 2^{-n} \end{aligned}$$

## Proving Fact 20(2)

Assume wlg. that  $1 \in (\mathcal{L}' \setminus \mathcal{L})$ .

$$\begin{aligned} & \Pr[R^{\mathcal{L}} = w \wedge R^{\mathcal{L}'} = w'] \\ &= \sum_{(t^2, \dots, t^\ell) \in \{0,1\}^{(\ell-1)n}} \Pr[(T^2, \dots, T^\ell) = (t^2, \dots, t^\ell)] \cdot \\ & \quad \Pr[R^{\mathcal{L}} = w \wedge R^{\mathcal{L}'} = w' \mid (T^2, \dots, T^\ell) = (t^2, \dots, t^\ell)] \\ &= \sum_{(t^2, \dots, t^\ell): (\oplus_{i \in \mathcal{L}} t^i) = w} \Pr[(T^2, \dots, T^\ell) = (t^2, \dots, t^\ell)] \\ & \quad \cdot \Pr[R^{\mathcal{L}'} = w' \mid (T^2, \dots, T^\ell) = (t^2, \dots, t^\ell)] \\ &= \sum_{(t^2, \dots, t^\ell): (\oplus_{i \in \mathcal{L}} t^i) = w} \Pr[(T^2, \dots, T^\ell) = (t^2, \dots, t^\ell)] \cdot 2^{-n} \\ &= 2^{-n} \cdot 2^{-n} \\ &= \Pr[R^{\mathcal{L}} = w] \cdot \Pr[R^{\mathcal{L}'} = w'] \end{aligned}$$



## Pairwise independence variables

### Definition 21 (pairwise independent random variables)

A sequence of random variables  $X^1, \dots, X^v$  is **pairwise independent**, if  $\forall i \neq j \in [v]$  and  $\forall a, b$ , it holds that

$$\Pr[X^i = a \wedge X^j = b] = \Pr[X^i = a] \cdot \Pr[X^j = b]$$

## Pairwise independence variables

### Definition 21 (pairwise independent random variables)

A sequence of random variables  $X^1, \dots, X^v$  is **pairwise independent**, if  $\forall i \neq j \in [v]$  and  $\forall a, b$ , it holds that

$$\Pr[X^i = a \wedge X^j = b] = \Pr[X^i = a] \cdot \Pr[X^j = b]$$

- By **Claim 20**,  $r^{\mathcal{L}}$  and  $r^{\mathcal{L}'}$  (chosen by **B**) are pairwise independent for every  $\mathcal{L} \neq \mathcal{L}' \subseteq [\ell]$ .



## Pairwise independence variables

### Definition 21 (pairwise independent random variables)

A sequence of random variables  $X^1, \dots, X^v$  is **pairwise independent**, if  $\forall i \neq j \in [v]$  and  $\forall a, b$ , it holds that

$$\Pr[X^i = a \wedge X^j = b] = \Pr[X^i = a] \cdot \Pr[X^j = b]$$

- By **Claim 20**,  $r^{\mathcal{L}}$  and  $r^{\mathcal{L}'}$  (chosen by **B**) are pairwise independent for every  $\mathcal{L} \neq \mathcal{L}' \subseteq [\ell]$ .
- Hence, also  $W^{\mathcal{L}}$  and  $W^{\mathcal{L}'}$  are.  
(Recall,  $W^{\mathcal{L}}$  is 1 iff  $A(f(x), r^{\mathcal{L}} \oplus e^j) \oplus b(x, r^{\mathcal{L}}) = x_j$ )

## Pairwise independence variables

### Definition 21 (pairwise independent random variables)

A sequence of random variables  $X^1, \dots, X^v$  is **pairwise independent**, if  $\forall i \neq j \in [v]$  and  $\forall a, b$ , it holds that

$$\Pr[X^i = a \wedge X^j = b] = \Pr[X^i = a] \cdot \Pr[X^j = b]$$

- By **Claim 20**,  $r^{\mathcal{L}}$  and  $r^{\mathcal{L}'}$  (chosen by **B**) are pairwise independent for every  $\mathcal{L} \neq \mathcal{L}' \subseteq [\ell]$ .
- Hence, also  $W^{\mathcal{L}}$  and  $W^{\mathcal{L}'}$  are.  
(Recall,  $W^{\mathcal{L}}$  is 1 iff  $A(f(x), r^{\mathcal{L}} \oplus e^j) \oplus b(x, r^{\mathcal{L}}) = x_j$ )

## Pairwise independence variables

### Definition 21 (pairwise independent random variables)

A sequence of random variables  $X^1, \dots, X^v$  is **pairwise independent**, if  $\forall i \neq j \in [v]$  and  $\forall a, b$ , it holds that

$$\Pr[X^i = a \wedge X^j = b] = \Pr[X^i = a] \cdot \Pr[X^j = b]$$

- By **Claim 20**,  $r^{\mathcal{L}}$  and  $r^{\mathcal{L}'}$  (chosen by **B**) are pairwise independent for every  $\mathcal{L} \neq \mathcal{L}' \subseteq [\ell]$ .
- Hence, also  $W^{\mathcal{L}}$  and  $W^{\mathcal{L}'}$  are.  
(Recall,  $W^{\mathcal{L}}$  is 1 iff  $A(f(x), r^{\mathcal{L}} \oplus e^j) \oplus b(x, r^{\mathcal{L}}) = x_j$ )

### Lemma 22 (Chebyshev's inequality)

Let  $X^1, \dots, X^v$  be pairwise-independent random variables with expectation  $\mu$  and variance  $\sigma^2$ . Then, for every  $\varepsilon > 0$ ,

$$\Pr \left[ \left| \frac{\sum_{j=1}^v X^j}{v} - \mu \right| \geq \varepsilon \right] \leq \frac{\sigma^2}{\varepsilon^2 v}$$

## B's success provability, cont.

Assuming that  $B$  always guesses  $\{b(x, t^i)\}$  correctly, then for every  $\mathcal{L} \subseteq [\ell]$

## B's success provability, cont.

Assuming that  $B$  always guesses  $\{b(x, t^i)\}$  correctly, then for every  $\mathcal{L} \subseteq [\ell]$

$$\triangleright \mathbb{E}[W^{\mathcal{L}}] \geq \frac{1}{2} + \frac{1}{q(n)}$$

## B's success provability, cont.

Assuming that **B** always guesses  $\{b(x, t^i)\}$  **correctly**, then for every  $\mathcal{L} \subseteq [\ell]$

- ▶  $E[W^{\mathcal{L}}] \geq \frac{1}{2} + \frac{1}{q(n)}$
- ▶  $\text{Var}(W^{\mathcal{L}}) := E[W^{\mathcal{L}}]^2 - E[(W^{\mathcal{L}})^2] \leq 1$

## B's success provability, cont.

Assuming that **B** always guesses  $\{b(x, t^i)\}$  **correctly**, then for every  $\mathcal{L} \subseteq [\ell]$

- ▶  $E[W^{\mathcal{L}}] \geq \frac{1}{2} + \frac{1}{q(n)}$
- ▶  $\text{Var}(W^{\mathcal{L}}) := E[W^{\mathcal{L}}]^2 - E[(W^{\mathcal{L}})^2] \leq 1$

## B's success provability, cont.

Assuming that **B** always guesses  $\{b(x, t^i)\}$  **correctly**, then for every  $\mathcal{L} \subseteq [\ell]$

- ▶  $E[W^{\mathcal{L}}] \geq \frac{1}{2} + \frac{1}{q(n)}$
- ▶  $\text{Var}(W^{\mathcal{L}}) := E[W^{\mathcal{L}}]^2 - E[(W^{\mathcal{L}})^2] \leq 1$

Taking  $\varepsilon = 1/2q(n)$  and  $v = 2n/\varepsilon^2$  (i.e.,  $\ell = \lceil \log(2n/\varepsilon^2) \rceil$ ), **Lemma 22** yields that

$$\Pr[m_i = x_i] = \Pr \left[ \frac{\sum_{\mathcal{L} \subseteq [\ell]} W^{\mathcal{L}}}{v} > \frac{1}{2} \right] \geq 1 - \frac{1}{2n} \quad (4)$$



## B's success provability, cont.

Assuming that **B** always guesses  $\{b(x, t^i)\}$  **correctly**, then for every  $\mathcal{L} \subseteq [\ell]$

- ▶  $E[W^{\mathcal{L}}] \geq \frac{1}{2} + \frac{1}{q(n)}$
- ▶  $\text{Var}(W^{\mathcal{L}}) := E[W^{\mathcal{L}}]^2 - E[(W^{\mathcal{L}})^2] \leq 1$

Taking  $\varepsilon = 1/2q(n)$  and  $v = 2n/\varepsilon^2$  (i.e.,  $\ell = \lceil \log(2n/\varepsilon^2) \rceil$ ), **Lemma 22** yields that

$$\Pr[m_i = x_i] = \Pr \left[ \frac{\sum_{\mathcal{L} \subseteq [\ell]} W^{\mathcal{L}}}{v} > \frac{1}{2} \right] \geq 1 - \frac{1}{2n} \quad (4)$$

## B's success provability, cont.

Assuming that **B** always guesses  $\{b(x, t^i)\}$  **correctly**, then for every  $\mathcal{L} \subseteq [\ell]$

- ▶  $E[W^{\mathcal{L}}] \geq \frac{1}{2} + \frac{1}{q(n)}$
- ▶  $\text{Var}(W^{\mathcal{L}}) := E[W^{\mathcal{L}}]^2 - E[(W^{\mathcal{L}})^2] \leq 1$

Taking  $\varepsilon = 1/2q(n)$  and  $v = 2n/\varepsilon^2$  (i.e.,  $\ell = \lceil \log(2n/\varepsilon^2) \rceil$ ), **Lemma 22** yields that

$$\Pr[m_i = x_i] = \Pr \left[ \frac{\sum_{\mathcal{L} \subseteq [\ell]} W^{\mathcal{L}}}{v} > \frac{1}{2} \right] \geq 1 - \frac{1}{2n} \quad (4)$$

Hence, by a union bound, **B** outputs  $x$  with probability  $\frac{1}{2}$ .

## B's success provability, cont.

Assuming that **B** always guesses  $\{b(x, t^i)\}$  **correctly**, then for every  $\mathcal{L} \subseteq [\ell]$

- ▶  $E[W^{\mathcal{L}}] \geq \frac{1}{2} + \frac{1}{q(n)}$
- ▶  $\text{Var}(W^{\mathcal{L}}) := E[W^{\mathcal{L}}]^2 - E[(W^{\mathcal{L}})^2] \leq 1$

Taking  $\varepsilon = 1/2q(n)$  and  $v = 2n/\varepsilon^2$  (i.e.,  $\ell = \lceil \log(2n/\varepsilon^2) \rceil$ ), **Lemma 22** yields that

$$\Pr[m_i = x_i] = \Pr \left[ \frac{\sum_{\mathcal{L} \subseteq [\ell]} W^{\mathcal{L}}}{v} > \frac{1}{2} \right] \geq 1 - \frac{1}{2n} \quad (4)$$

Hence, by a union bound, **B** outputs  $x$  with probability  $\frac{1}{2}$ .

## B's success provability, cont.

Assuming that **B** always guesses  $\{b(x, t^i)\}$  **correctly**, then for every  $\mathcal{L} \subseteq [\ell]$

- ▶  $E[W^{\mathcal{L}}] \geq \frac{1}{2} + \frac{1}{q(n)}$
- ▶  $\text{Var}(W^{\mathcal{L}}) := E[W^{\mathcal{L}}]^2 - E[(W^{\mathcal{L}})^2] \leq 1$

Taking  $\varepsilon = 1/2q(n)$  and  $v = 2n/\varepsilon^2$  (i.e.,  $\ell = \lceil \log(2n/\varepsilon^2) \rceil$ ), **Lemma 22** yields that

$$\Pr[m_i = x_i] = \Pr \left[ \frac{\sum_{\mathcal{L} \subseteq [\ell]} W^{\mathcal{L}}}{v} > \frac{1}{2} \right] \geq 1 - \frac{1}{2n} \quad (4)$$

Hence, by a union bound, **B** outputs  $x$  with probability  $\frac{1}{2}$ .

Taking the guessing into account, yields that **B** outputs  $x$  with probability at least  $2^{-\ell}/2 \in \Omega(n/q(n)^2)$ .

- Hardcore functions:  
Similar ideas allows to output  $\log n$  “pseudorandom bits”

# Reflections

- Hardcore functions:

Similar ideas allows to output  $\log n$  “pseudorandom bits”

- Alternative proof for the LHL:

Let  $X$  be a rv with over  $\{0, 1\}^n$  with  $H_\infty(X) \geq t$ , and assume  $SD((R_n, \langle R_n, X \rangle_2), (R_n, U_1)) > \alpha = 2^{-c \cdot t}$  for some universal  $c > 0$ .

# Reflections

- Hardcore functions:

Similar ideas allows to output  $\log n$  “pseudorandom bits”

- Alternative proof for the LHL:

Let  $X$  be a rv with over  $\{0, 1\}^n$  with  $H_\infty(X) \geq t$ , and assume  $SD((R_n, \langle R_n, X \rangle_2), (R_n, U_1)) > \alpha = 2^{-c \cdot t}$  for some universal  $c > 0$ .

# Reflections

- Hardcore functions:

Similar ideas allows to output  $\log n$  “pseudorandom bits”

- Alternative proof for the LHL:

Let  $X$  be a rv with over  $\{0, 1\}^n$  with  $H_\infty(X) \geq t$ , and assume  $SD((R_n, \langle R_n, X \rangle_2), (R_n, U_1)) > \alpha = 2^{-c \cdot t}$  for some universal  $c > 0$ .

$\implies$  Exists (a possibly inefficient) algorithm  $D$  that distinguishes  $(R_n, \langle R_n, X \rangle_2)$  from  $(R_n, U_1)$  with advantage  $\alpha$



# Reflections

- Hardcore functions:

Similar ideas allows to output  $\log n$  “pseudorandom bits”

- Alternative proof for the LHL:

Let  $X$  be a rv with over  $\{0, 1\}^n$  with  $H_\infty(X) \geq t$ , and assume  $SD((R_n, \langle R_n, X \rangle_2), (R_n, U_1)) > \alpha = 2^{-c \cdot t}$  for some universal  $c > 0$ .

$\implies$  Exists (a possibly inefficient) algorithm  $D$  that distinguishes  $(R_n, \langle R_n, X \rangle_2)$  from  $(R_n, U_1)$  with advantage  $\alpha$

$\implies$  Exists algorithm  $A$  that predicts  $\langle R_n, X \rangle_2$  given  $R_n$  with prob  $\frac{1}{2} + \alpha$

# Reflections

- Hardcore functions:

Similar ideas allows to output  $\log n$  “pseudorandom bits”

- Alternative proof for the LHL:

Let  $X$  be a rv with over  $\{0, 1\}^n$  with  $H_\infty(X) \geq t$ , and assume  $SD((R_n, \langle R_n, X \rangle_2), (R_n, U_1)) > \alpha = 2^{-c \cdot t}$  for some universal  $c > 0$ .

$\implies$  Exists (a possibly inefficient) algorithm  $D$  that distinguishes  $(R_n, \langle R_n, X \rangle_2)$  from  $(R_n, U_1)$  with advantage  $\alpha$

$\implies$  Exists algorithm  $A$  that predicts  $\langle R_n, X \rangle_2$  given  $R_n$  with prob  $\frac{1}{2} + \alpha$

$\implies$  (by GL) Exists algorithm  $B$  that guesses  $X$  from nothing, with prob  $\alpha^{O(1)} > 2^{-t}$

## Reflections cont.

- List decoding:

An encoder  $C: \{0, 1\}^n \mapsto \{0, 1\}^m$  and a decoder  $D$ , such that the following holds for any  $x \in \{0, 1\}^n$  and  $c$  of hamming distance  $\frac{1}{2} - \delta$  from  $C(x)$ :

## Reflections cont.

- List decoding:

An encoder  $C: \{0, 1\}^n \mapsto \{0, 1\}^m$  and a decoder  $D$ , such that the following holds for any  $x \in \{0, 1\}^n$  and  $c$  of hamming distance  $\frac{1}{2} - \delta$  from  $C(x)$ :

## Reflections cont.

- List decoding:

An encoder  $C: \{0, 1\}^n \mapsto \{0, 1\}^m$  and a decoder  $D$ , such that the following holds for any  $x \in \{0, 1\}^n$  and  $c$  of hamming distance

$\frac{1}{2} - \delta$  from  $C(x)$ :

$D(c, \delta)$  outputs a list of size at most  $\text{poly}(1/\delta)$  that whp. contains  $x$

## Reflections cont.

- List decoding:

An encoder  $C: \{0, 1\}^n \mapsto \{0, 1\}^m$  and a decoder  $D$ , such that the following holds for any  $x \in \{0, 1\}^n$  and  $c$  of hamming distance  $\frac{1}{2} - \delta$  from  $C(x)$ :

$D(c, \delta)$  outputs a list of size at most  $\text{poly}(1/\delta)$  that whp. contains  $x$

The code we used here is known as the **Hadamard** code

## Reflections cont.

- List decoding:

An encoder  $C: \{0, 1\}^n \mapsto \{0, 1\}^m$  and a decoder  $D$ , such that the following holds for any  $x \in \{0, 1\}^n$  and  $c$  of hamming distance  $\frac{1}{2} - \delta$  from  $C(x)$ :

$D(c, \delta)$  outputs a list of size at most  $\text{poly}(1/\delta)$  that whp. contains  $x$

The code we used here is known as the **Hadamard** code

- LPN - learning parity with noise:

Find  $x$  given polynomially many samples of  $\langle x, R_n \rangle_2 + N$ , where  $\Pr[N = 1] \leq \frac{1}{2} - \delta$ .

## Reflections cont.

- List decoding:

An encoder  $C: \{0, 1\}^n \mapsto \{0, 1\}^m$  and a decoder  $D$ , such that the following holds for any  $x \in \{0, 1\}^n$  and  $c$  of hamming distance  $\frac{1}{2} - \delta$  from  $C(x)$ :

$D(c, \delta)$  outputs a list of size at most  $\text{poly}(1/\delta)$  that whp. contains  $x$

The code we used here is known as the **Hadamard** code

- LPN - learning parity with noise:

Find  $x$  given polynomially many samples of  $\langle x, R_n \rangle_2 + N$ , where  $\Pr[N = 1] \leq \frac{1}{2} - \delta$ .

The difference comparing to Goldreich-Levin – no control over the  $R_n$ 's.